A B S T R A C T

The present invention relates to a security token and method for secure usage of digital certificates and related keys on a security token, and more particularly, a secure import of certificates into a security token and their secure usage by applications. The root certificate of the certification authority(CA) is used during the initialization of the security token in a secure environment to transfer the certified root public key of the CA and its attributes into the data structure of the security token. The public root key is write protected. Furthermore, a verification component, preferably part of the operating system of the security token will accept, in case the certificate has to be replaced, only user certificates having a valid digital signature by the private root key of the CA.